REMARKS

The present invention is a method and system comprising a terminal, including a display and a network, the terminal using a browser to communicate with a network during a terminal session comprising at least one communication operation initiated by a user and transmits the network, and a system comprising a terminal including a display, a network including a server, to which the terminal is coupled by a telecommunications link, a mobile terminal and a program executable on a processor in a system comprising a terminal, including a display in a network, the terminal using a browser to communicate with a network during a terminal session comprising at least one communication operation initiated by a user and transmitted to the network. In a system comprising a terminal, including a display in a network, the terminal using a browser to communication with the network during a terminal session comprising at least one communication operation initiated by a user and transmitted to the network, a method in accordance with the embodiment of the invention that includes initiating a terminal session with a browser by making a transmission to the network; the network, in response to initiation of the terminal session, providing information from the network to the browser relating to the terminal session; displaying on the display a level of trust, informing the user of a level of security to be determined associated with the communication operation of at least one communication operation is permitted by the user to be transmitted to the network based upon a comparison of the at least one communication operation to the standard prior to transmission to the network and wherein based upon the displayed level of trust, the user decides to accept or reject the at least one communication operation as a result of the comparison.

Claim 1-40, 43-83 and 86-95 stand rejected under 35 U.S.C. §103 as being unpatentable over United States Patent 5,958,051 (Renaud et al). These grounds of rejection are traversed with respect to claims 1 and 43 for the following reasons.

In the first place, Renaud et al disclose a method, apparatus and product for establishing and verifying authenticity of data within one or more data files. Renaud et al's process sets security levels in a security manager as illustrated in Fig. 5. Security levels are considered to be levels of trust which vary from high security level to low security level as discussed in column 10, lines 8-67, through column 11, lines 1-45.

Renaud et al's processing is fundamentally different than that of the subject matter set forth in claims 1 and 43 in that, in accordance with the claimed invention, displaying of a level of trust is utilized to inform the user of a level of security determined to be associated with at least one communication operation if the at least one communication operation is permitted by the user to be transmitted to a network based upon a comparison of the at least one communication operation to a standard prior to transmission prior to the network. Based upon the displayed level of trust, the user decides whether to accept or reject the at least one communication operation as a result of the comparison. This mode of operation is not disclosed by Renaud et al.

As stated above, while Renaud et al does determine levels of trust, there is no display of a security level upon which a decision of whether to connect to a network is made. In this regard, it is noted that the Examiner alludes to there being a display of level of trust with the Examiner citing column 10, lines 25-62 and column 12, lines 40 through column 13, line 45. However, it is submitted that those portions

do not describe the display of a level of trust utilized by the user to determine whether connectivity to a network is permitted. Instead, what is described is the processing of security levels for software, such as permitting applets to be executed. This process is not dependent upon user intervention as claimed. See, for example, column 13, lines 25-40, wherein when the security settings are satisfied, the applet action is allowed to happen at step 620. Accordingly, it is submitted that there is a fundamental difference between Renaud et al and claims 1 and 43 which is that Renaud et al's process does not pertain to the control of communications between a terminal and a network wherein the user in response to a displayed level of trust determines whether the at least one communication operation is permitted. There is no basis in the record why a person of ordinary skill in the art would be led to modify the teachings of Renaud et al to arrive at the subject mater of claims 1 and 43.

Moreover, the dependent claims 2-42 and 45-85 define further aspects of the present invention which are not rendered obvious by Renaud et al.

Claim 86 recites:

> A system comprising:
> a terminal including a display;
> a network including a server to which the terminal is coupled by a telecommunications link; and wherein
> the server stores a certificate issued by a trusted third party containing a verified identity of the server or an organization responsible for the server and a secret key, the secret key and the certificate, being transmitted to the terminal and processed by the terminal to determine if the identify of the server may be displayed to a user of the terminal as being from a trusted source, the display containing at least one page containing frames and a display indicating whether the frames are certified as being from a trusted source.

and claim 89 recites:

> A method in a system comprising a terminal including a display, a network including a server to which the terminal is coupled by a telecommunications link, the method comprising:
>
> storing with the server a certificate issued by a trusted third party containing a verified identity of the server or an organization responsible for the server and a secret key;
>
> transmitting the certificate and the secret key to the terminal; and
>
> processing at the terminal the certificate and the key to determine if the identity of the server may be displayed to the user of the terminal as being a trusted source; and
>
> displaying with the display results of the processing.

The Examiner concludes:

> Per claims 86-91, it is noted that the use of key pair (public key and private key) issued by a third party authority for verifying a source file is well known in the art (see Renaud in col 2, lines 1-17)
>
> Renaud does not explicitly teach maintaining a secret key at the server and transmitting a public key to the user terminal.
>
> It would have been obvious to one of ordinary skill in the art at the time the invention was made to realize such use of key pair in Renaud's verification step because it would have enabled the user terminal to securely verifying the source file and the site certificate (see Renaud in col 12, lines 53-65)

The Examiner's reasoning regarding a key pair does not address the scope of claims 86 and 89. The claims each recite storing a certificate issued by a trusted third party containing a verified identity of the server organization responsible for the server and a public key, the public key being transmitted to the terminal and processed by the terminal to determine if the identity of the server may be displayed to a user of the terminal as being from a trusted source, the display containing at least one page containing frames and a display indicating whether the frames are

certified as being from a trusted source. The Examiner's rationale does not address the scope of claims 86 and 89 as discussed above.

Claim 92 recites:

> A mobile terminal comprising:
> a user display; and
> a browser which indicates on the user display a level of trust, based upon a comparison of at least one communication operation involving the mobile terminal and a network coupled thereto to a standard and informing a user of a security level determined to be associated with the at least one communication operation.

and claim 94 recites:

> In a mobile terminal having a processor and a user display, a program executable on the processor which is downloadable thereto from a network coupled to the mobile terminal, the program causing the user display to display a level of trust, based upon comparison of at least one communication operation involving the mobile terminal and a network coupled thereto to a standard and informing the user of a security level determined to be associated with the at least one communication operation.

It is noted that the Examiner concludes that "[c]laims 43-83 and 92-95 are similar in scope as to that of claims 1-40. However, it is submitted that the Examiner's rationale is erroneous since, as pointed out above, Renaud et al do not display a level of trust based upon a comparison of at least one communication operation involving the mobile terminal and a network coupled thereto to a standard and informing the user of a security level determined to be associated with the at least one communication operation between a mobile terminal and a network.

Claims 41-42 and 84-85 stand rejected under 35 U.S.C. §103 as being unpatentable over Renaud et al in view of United States Patent 5,953,528 (Sullivan).

The Examiner reasons as follows:

> Renaud's teachings are still applied as discussed above. Renaud does not teach using numerical rating or graphical indicators to display the trust levels. Sullivan discloses using graphical indicators to display different trust levels (see Sullivan's col 6, lines 2-6)
>
> It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize numerical rating or graphical indicators to display different trust levels in Renaud because it would have enabled users to more easily visualize different levels of trust associated with the web sites and/or data files.

These grounds of rejection are traversed for the following reasons.

While Sullivan does disclose a server 12 which maintains levels of trust of a knowledge object 22 in which each level of confidence is associated with a color and an identifiable graphical stamp that is affixed to the knowledge object, such teaching would not be considered by a person of ordinary skill in the art to be combinable with Renaud et al to meet the subject matter of claims 41, 42, 84 and 85 since, as pointed out above, Renaud et al does not even consider making a decision to accept or reject at least one communication operation based upon a displayed level of trust. Therefore, a person of ordinary skill in the art would not consider combining Sullivan with Renaud et al to utilize a numerical rating or graphical indicator to display levels of trust without impermissible hindsight.

In view of the foregoing amendments and remarks, it is submitted that each of the claims in the application is in condition for allowance. Accordingly, early allowance thereof is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 C.F.R. §1.136. Please charge any shortage in fees due in connection with the

filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (0171.40111X00) and please credit any excess fees to such Deposit Account.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Donald E. Stout
Registration No. 26,422
(703) 312-6600

DES:dlh